		Business Objective: Provide Security And Disaster Recovery Requirements To Enable And Maintain Continuous 24/7 BOE Business Operations And Service Mid-Level Solution Requirements:	Tax Program		Business Capability/Function Serviced	PRIORITY (Mandatory, Desirable Scored)
			Private Rail Car (PRC)	Board Roll		
11.01		Solutions hosted in either Amazon Web Services (AWS) or Microsoft Azure, must comply with the State Cloud Computing Policy, State Administrative Manual (SAM) Sections 4983-4983.1	x	x	Security	Mandatory
11.02		Contractor must indicate whether solution includes Generative AI (GenAI) components and, if so, complete the State Generative Artificial Intelligence Risk Assessment from Statewide Information Management Manual (SIMM) 5305-F.	x	x	Security	Mandatory
11.03		Contractor must indicate whether solution will be implemented via re-hosting (lift-and-shift), re-factoring (lift, tinker and shift) or re-factoring (re-architecting) cloud architecture.	x	x	Security	Mandatory
11.04		Contractor shall prepare, deliver and maintain all documentation required by the California Department of Technology (CDT) for cloud system approval, including but not limited to the sections below. *This review is expected to take 14 business days. If documentation is missing or inadequate, the review may take longer.*	x	x	Security	Mandatory
	11.04.1	California Cloud Services Assessment (CCSA) Questionaire from the CCSA guide, Statewide Information Management Manual (SIMM) 141.	x	x	Security	Mandatory
	11.04.2	Contractor shall design the solution with an exit strategy from the Cloud Solution Provider/tenant as indicated in the California Cloud Services Assessment (CCSA) Questionaire to include but not limited to, configure a dedicated subscription or account under State ownership with no dependency on contractor-owned tenants, organizations or identies. Deploy all resources into dedicated, isolated network environments within the subscription or account. No peering, shared subnets or cross subscription/cross account connectivity unless explicity approved in writing by BOE. Federated to Entra ID tenant for identity and group-based access management. Separate storage, databases, and key management services for each subscription or account. No shared data repositiories or encyrption keys. Contractor shall provide comprehensive documentation of all resources, dependencies, configurations, identity mappings, networking, firewall and routing configurations, data storage locations and encryption key ownership.	x	x	Security	Mandatory
	11.04.3	Cloud Alternative Analysis from the CCSA guide, Statewide Information Management Manual (SIMM) 141.	x	x	Security	Mandatory
	11.04.4	1) Cloud Architecture & 2) Network Diagrams for solution from the CCSA guide, Statewide Information Management Manual (SIMM) 141.	x	x	Security	Mandatory
	11.04.5	Roles and Responsibilities Matrix identifying agency, contractor, and cloud service provider responsibilities.	x	x	Security	Mandatory
	11.04.6	Privacy Threshold Assessment and Privacy Impact Assessment from the Statewide Information Management Manual (SIMM) 5310-C.	x	x	Security	Mandatory
	11.04.7	Classification Categorization Form – System Classification (FIPS 199) from the Statewide Information Management Manual (SIMM) 141	x	x	Security	Mandatory
	11.04.8	Well-Architected Framework Assessment or equivalent from Cloud Service Provider for review.	x	x	Security	Mandatory
	11.04.9	Cloud System Security Plan (CSSP) for solution from CDT's California Cloud Services Assessment webpage.	x	x	Security	Mandatory
	11.04.10	Contractor shall provide all documentation necessary to incorporate the solution into the Technology Recovery Plan (TRP) including but not limited to, recovery procedures, RTOs, RPOs, dependencies, failover mechanisms and evidence of recovery testing per Statewide Information Management Manual (SIMM) 5325-A.	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.04.11	Solution must align to Cloud Security Standard from the Statewide Information Management Manual (SIMM) 5315-B and Cloud Security Guide (SIMM) 140.	x	x	Security	Mandatory
	11.04.12	Solution must align with the National Institute of Standards and Technology (NIST) 800-207 Zero Trust Architecture	x	x	Security	Mandatory
11.05		The Solution, and all data, must be hosted within the USA, and all accesses, and support of the systems and services are performed from the United States, its possessions, and territories.	x	x	Security	Mandatory
11.06		The solution must encrypt data in transit and at rest and must comply with the latest version of Federal Information Processing Standards (FIPS) cryptography and California State Administrative Manual (SAM) 5350.1.	x	x	Security	Mandatory
11.07		The system must keep confidential, sensitive or Personally Identifiable Information (PII) encrypted in accordance with California State Administrative Manual (SAM) 5350.1.	x	x	Security	Mandatory

		Business Objective: Provide Security And Disaster Recovery Requirements To Enable And Maintain Continuous 24/7 BOE Business Operations And Service Mid-Level Solution Requirements:	Tax Program		Business Capability/Function Serviced	PRIORITY (Mandatory, Desirable Scored)
			Private Rail Car (PRC)	Board Roll		
11.08		Security standards must meet the additional requirements:	x	x	Security	Mandatory
	11.08.1	All employees, contractors, or subcontractors must perform the work within the USA or one of its territories.	x	x	Security	Mandatory
	11.08.2	The contractor shall comply with the California State Administrative Manual (SAM) 5305.1 by implementing and maintaining appropriate administrative, technical, and physical safeguards to protect State information assets, and shall adhere to the California Department of Technology (CDT) Information Security Contract Clause, including requirements to maintain security controls consistent with State and federal standards, protect State data from unauthorized access, use, disclosure, disruption, modification, or destructions, report security incidents within required timeframes, and ensure subcontractors handling State data are bound by the same obligations.	x	x	Security	Mandatory
	11.08.3	The contractor must ensure the solution complies with CDT logging forwarding standards for all cloud workload logs, including virtual machines, services and applications for CDT SOCaaS requirements for continuous monitoring.	x	x	Security	Mandatory
	11.08.4	The contractor assumes responsibility for the security and confidentiality of the data under its control.	x	x	Security	Mandatory
	11.08.5	No data must be copied, modified, destroyed, or deleted by the Contractor other than for normal operation or maintenance of SaaS during the Contract period without prior written notice to and written approval by the State.	x	x	Security	Mandatory
	11.08.6	Confidential, sensitive, or personally identifiable information must be encrypted in accordance with California State Administrative Manual 5350.1 and California Statewide Information Management Manual 5305-A.	x	x	Security	Mandatory
	11.08.7	The data must be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).	x	x	Security	Mandatory
	11.08.8	The contractor shall utilize the designated Identity Provider (Microsoft Entra ID) for authentication and access to solution and shall ensure all contractor personnel comply with the State's identity and access management policies, including multi-factor authentication requirements according to Statewide Information Management Manual (SIMM) 5360-C.	x	x	Security	Mandatory
	11.08.9	The solution must provide the ability to produce a “warning banner” with acceptance that warns authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s).	x	x	Security	Mandatory
11.09		In the event of disaster or catastrophic failure that results in significant data loss or extended loss of access to data, Contractor must notify the State by the fastest means available and in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency. Contractor must provide such notification within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contractor must inform the State of:	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.09.1	The scale and quantity of the data loss.	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.09.2	What Contractor has done or will do to recover the data and mitigate any deleterious effect of the data loss.	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.09.3	What corrective action Contractor has taken or will take to prevent future data loss. What corrective action Contractor has taken or will take to prevent future data loss.	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.09.4	If Contractor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.09.5	Contractor must restore continuity, restore data in accordance with the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) as set forth in the Service Level Agreement (SLA), restore accessibility of data, and repair as needed to meet the performance requirements stated in the SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.	x	x	Disaster Recovery/Business Continuity	Mandatory
	11.09.6	Contractor must conduct an investigation of the disaster or catastrophic failure and must share the report of the investigation with the State to include root cause analysis. The State and/or its authorized agents must have the right to lead (if required by law) or participate in the investigation. Contractor must cooperate fully with the State, its agents and law enforcement.	x	x	Disaster Recovery/Business Continuity	Mandatory